ANÁLISIS Y DESARROLLO DE ESTRATEGIAS PARA LA PREVENCIÓN DEL USO DE LA INGENIERÍA SOCIAL EN LA SOCIEDAD DE LA INFORMACIÓN

Oscar David López Villa
Universidad de San Buenaventura Medellín
oscarlopez.v86@gmail.com

Wilmar Darío Restrepo Gil
GAULA - Policía Nacional de Colombia
wilres72@yahoo.es

(Tipo de Artículo: **Reflexión**. Recibido el 17/07/2013. Aprobado el 09/12/2013)

RESUMEN
La Ingeniería Social se podría definir como aquellas estrategias y técnicas que se usan para obtener información de las personas.
Para entender cómo afecta a un sistema e incluso a nosotros mismos, se tienen 2 escenarios: el primero es donde el ingeniero social interactúa con una posible victima mediante diversas formas (e-mail, llamadas telefónicas, sms, llamar directamente a la persona), usando la persuasión, engaño y en algunos casos las amenazas, para obtener información privilegiada de un sistema que él quiere atacar pero usando a las personas como un medio para hacerlo; el segundo es donde el ingeniero social piensa en las personas como su objetivo principal usando las mismas formas y técnicas ya mencionadas pero no está buscando información de ellas, más bien lo que lo impulsa es el dinero usando sus habilidades para enriquecerse a costa de otros.

Palabras clave
Ataque, explotación, riesgo, tecnología.

ANALYSIS AND DEVELOPMENT OF STRATEGIES FOR PREVENTING THE USE OF SOCIAL ENGINEERING IN THE INFORMATION SOCIETY

ABSTRACT
Social Engineering can be defined as those strategies and techniques used to obtain information from people.

In order to understand how social engineering affects a system and even how it affects ourselves, there are two scenarios: the first is where the social engineer interacts with a potential victim in different ways (e-mail, phone calls and short message services), using persuasion, fraud and threats in some cases, to obtain inside information of a system he wants to attack but using people as a means to do it, the second one is where the social engineer thinks of people as their main objective using the same forms and techniques mentioned above but he is not looking information of them, instead of that what drives him is the money using their skills to enrich themselves at the expense of others.

Keywords
Attack, exploitation, risk, technology.

ANALYSE ET DÉVELOPPEMENT DES STRATÉGIES POUR PRÉVENIR L'USAGE DE L'INGÉNIERIE SOCIALE DANS LA SOCIETÉ DE L'INFORMATION

RÉSUMÉ
L'ingénierie sociale peut être définie comme l'ensemble des stratégies et techniques qui sont utilisés pour obtenir l'information des personnes.

Pour comprendre la manière comme l'ingénierie sociale affecte un système et comme nos affecte on a deux scénarios : Le premier est celui quand l'ingénieur social interagit avec une victime potentielle au moyen de différents communications (émail, appels téléphoniques et service d'envoie de messages courts), en utilisant persuasion, tromperie, et dans quelques cas en utilisant des menaces pour obtenir information privilégiée d'un système que l'ingénieur social veut attaquer mais en s'appuyant sur les personnes comme un moyen pour cela ; le second scénario est celui où l'ingénieur social considère les personnes comme son objectif principal en utilisant les mêmes formes et techniques qu'on a déjà mentionné mais, dans ce cas, il ne cherche pas leur information, ce qu'il cherche c'est l'argent en utilisant ses habiletés pour s'enrichir aux dépens des autres.

Mots-clés
Attaque, exploitation, risque, technologie.

INTRODUCCIÓN

Desde hace mucho tiempo las personas han usado sus habilidades de comunicación y convencimiento para obtener lo que desean de otras personas y al mismo tiempo haciéndolas sentir que están haciendo lo correcto.

Con el surgimiento de las nuevas tecnologías de la información, como el correo electrónico y más recientemente las redes sociales, esta tarea se ha hecho mucho más fácil para los delincuentes informáticos ya que al aumentar la cantidad de posibles víctimas se incrementa la probabilidad de tener éxito en su intento de capturar información de los usuarios de internet.

Al mismo tiempo que nacen estas nuevas tecnologías también aparecen nuevas técnicas como: el robo de dinero mediante el uso del correo electrónico utilizando el nombre de entidades bancarias o cualquier entidad prestadora de servicios; de igual forma se comete este delito mediante el envío de mensajes de texto (SMiShing), informándole a la posible victima que ha ganado un premio y es necesario enviar información por este mismo medio o en ocasiones hacer recargas a números de celulares para hacer efectiva la entrega del premio.

Otra técnica muy utilizada en el mundo de la ingenia social es el robo de información personal por los medios mencionados anteriormente, añadiéndole el uso de llamadas telefónicas a sus posibles víctimas para solicitarles información con alguna excusa como que han tenido un percance con la base de datos de la empresa con la cual esta vincula mediante un servicio y necesitan unos datos para corregirlo

1. ATACANDO UN SISTEMA

Para que un ataque informático se defina como exitoso se requieren 5 fases, pero se entrara en más detalles en la fase de reconocimiento por que es aquí donde la ingeniería social se destaca.

Fase 1: Reconocimiento (Footprinting).

Con el reconocimiento se pretende recolectar toda la información posible que sea pública de la víctima o de fácil acceso y para hacer esto el atacante utiliza varias herramientas:

Lo primero de su lista son los buscadores (google, bing, shodanhq) [1], con ellos puede encontrar registros telefónicos con nombres a quien pertenecen, documentos públicos y otros no tanto, nombres de usuario y contraseña, empresas aliadas, direcciones IP, whois [2] y un largo etc.

Otra herramienta disponible es la Ingeniería social donde al interactuar con un usuario del sistema puede obtener mucha información ya mencionada anteriormente, incluso si es bueno puede simplemente saltarse todas las fases y controlar todo el sistema con una llamada.

Fase 2: Exploración (Fingerprinting).

En esta etapa se usa toda la información obtenida en la fase 1, la fase 2 se caracteriza por obtener información sobre rangos de direcciones IP, nombre de host, servicios que presta (ftp, web, almacenamiento de archivos, videos, música), escaneo de puertos [3], y escaneo de vulnerabilidades; su principal diferencia con la fase de reconocimiento está en que busca información de una forma más directa sobre el objetivo mientras que la fase anterior se centra solo en la información contenida en la red (google, bing, shodan).

Fase 3: Obteniendo el acceso.

Aquí se logra entrar al sistema y para eso esto el atacante se vale de explotar vulnerabilidades encontradas en la fase 2 como también claves débiles o por defecto.

Fase 4: Manteniendo el acceso.

Una vez ya adentro del sistema el atacante instala programas como sniffers [4] que le permiten capturar contraseñas del sistema, sesiones FTP [5] y telnet [6], o puede instalar troyanos [7] que le ayudaran a entrar posteriormente sin ningún problema.

Fase 5: Borrado de huellas.

En esta fase el atacante hace todo lo posible por destruir toda evidencia de sus actos con el único fin de ocultar sus actividades y tener por más tiempo el control del sistema sin ser descubierto.

3. KEVIN MITNICK USANDO LA INGENIERÍA SOCIAL

Él hacker Kevin Mitnick fue en sus mejores tiempos el mejor hacker y phreaker (hacker de la telefonía) del mundo hasta el punto de la exageración suponiendo que “solo con tener acceso a un teléfono podría hacer estallar la tercera guerra mundial”.

El Cóndor como fue reconocido en la comunidad hacker, nunca fue reconocido por sus habilidades técnicas ni tecnológicas frente a un sistema; él hacía alusión de que sin importar cuán segura fuese una infraestructura y sin importar sus protocolos de seguridad, siempre habrá alguien, un ser humano usándolo o administrándolo, esto con el afán de decir que el eslabón más débil de la cadena, son las personas.

En varias ocasiones (1981, 1983, 1987, 1995) Kevin Mitnick estuvo en prisión por lograr obtener credenciales y acceso a sistemas del gobierno, compañías de telefonía fija y móvil usando como su principal herramienta la "ingeniería social" llamando directamente al personal de la empresa, preguntando por credenciales de acceso y/o el procedimiento que debía seguir para hacerlo.

Luego de los tropiezos que tuvo con la policía y al salir de prisión se dedicó a consultoría y el asesoramiento en materia de seguridad, también escribió 2 libros en los que trata el tema de la ingeniera social el primero el "the art of deception" y el segundo "el arte de la intrusión" donde habla de forma extensa del tema mediante experiencias de hackers sobre ataque reales.

4. ANTECEDENTES

A. Segu-Info

En el año 2011, la página segu-info [8] que se especializa en temas de seguridad de la información en argentina realizo durante 2 meses una encuesta sobre el phishing a 1.314 usuarios centrándose en como las personas lo percibían y si sabrían diferenciarlo del spam y el scam.

La primero pregunta fue si sabían reconocer un caso de phishing, donde alrededor del 68% respondieron afirmativamente; se percibe que muchos de los usuarios creen estar protegidos frente a estos ataques siendo una desventaja en sí misma, se hizo evidente que no reconocían la diferencia en respuestas como en la cuales identificaban el phishing mirando si el correo no tenía un buen aspecto visual, o sea que si el correo es bonito es de fiar o donde ofrecían productos farmacéutico lo cual se clasifica como spam o scam.

Otra pregunta fue "¿Qué hace cuando lo recibe?", 2 personas lo responden y unas 66 miran siguiendo los enlaces contenidos en los correos. Las personas que se dedican a enviar este tipo de correos cuentan con esas 2 personas que solo representan el 0,15% del total, pero que pasa si son 10.000, 100.000 o 500.000 correos, además esas 66 pueden sufrir otro tipo de ataque (descarga de malware, infección de código, clickjacking), en donde se infecten sus equipos y robar sus datos personales, así que se puede hablar de alrededor de unas 70 personas por cada 1300 correos.

El 78% de los encuestados asegura no saber dónde hacer la denuncia de estos casos, asegurando que este tipo de fraude continúe circulando en la red.

B. AV-Comparatives

AV-Comparatives [9] realizó una encuesta sobre seguridad informática pero con un enfoque en el uso de antivirus. La encuesta tuvo una duración de 30 días en los cuales unos 4.715 usuarios la respondieron.

Principales hallazgos:

- "Alrededor del 3% de los usuarios no usa antivirus"

Esto puede deberse a que el antivirus puede ser molesto, con muchas alertas o muchos mensajes de actualizaciones, también puede causar un bajo rendimientos debido a que no posee la capacidad suficiente de ejecutar este programa.

- "La mayoría de los usuarios (70%) no contacta al fabricante cuando encuentra un falso positivo o el producto no detecta algo que debería detectar."

No es fácil detectar cuando el antivirus se equivoca, para reconocer esto es necesario tener cierto nivel de conocimientos frente a la tema.

- "A la mayoría de los usuarios le importa tanto la detección (73%) como la performance del producto (27%)"

Si el programa es complicado de manejar o no se entiende cuáles son sus funciones, se optara por un producto que si tenga estas características, por lo tanto los fabricantes de antivirus se esfuerzan por hacer un producto confiable y la vez fácil de manejar.

- "La mitad (55%) de los usuarios utiliza productos antivirus pagos, lo cual representa un decrecimiento importante respecto a la encuesta de 2012."

Los antivirus de pago no son mucho mejores en comparación con la versión gratuita del mismo fabricante en cuanto a protección contra virus se refiere, pero lo que si ofrecen son una serie de módulos que permiten analizar el correo electrónico, las descargas y algunas veces código malicioso que quiere infiltrarse cuando se navega en la red, además ofrece actualizaciones más rápidas cuando se descubre algún tipo de malware [10] que represente una gran amenaza.

5. EL INGENIERO SOCIAL

Actualmente las empresas gastan mucho dinero en sus infraestructuras como IDS (sistemas de detector de intrusos), IPS (sistemas de prevención de intrusos), firewalls, sistemas de encriptación de datos, tanto en el equipo como en la red, pero es poca la inversión que están haciendo en la creación de cultura de seguridad informática, los ingenieros sociales lo saben muy bien y usan todas sus habilidades para crear situaciones con las que consigan la información que desean:

Credibilidad
El ingeniero social debe hacer que su posible victima confié en él, este es un paso casi obligatorio si quiere lograr su objetivo.

Esta el escenario done el ingeniero social se comunica con su víctima mediante el teléfono*, buenos días soy de la empresa ABC y acabamos de hacer una actualización del sistema, estamos llamando a nuestros clientes para saber si tienen servicio de internet, a lo cual la victima responde que no (el delincuente causa el daño) entonces necesito unos datos para restablecer el servicio: por favor deme su nombre y su número de cedula para verificarlo en el sistema, muy bien, ahora el nombre de usuario y clave de acceso a su computador*, luego de obtener los datos restablece la conexión para no levantar sospechas.

Los rasgos de un rol
Aquí el ingeniero social suplanta la identidad de una persona con poder: se puede suponer el escenario en donde el "jefe" se comunica con un "subalterno" y le pide el usuario y contraseña de acceso al servidor "xcvd".

Lo que el ingeniero social hizo fue pedir unos datos del servidor, a lo que empleado responde porque solamente alguien que sepa el nombre del servidor debe ser de la empresa.

El deseo de ayudar
Las personas siempre están prestas ayudar y esto es aprovechado por el ingeniero social haciéndose pasar por un usuario que llama a alguien de soporte técnico informando que es incapaz de iniciar sesión en su equipo y necesita ayuda para resolver su problema.

Miedo
El miedo es uno de los métodos más comunes y utilizado por los delincuentes como en los casos de phising [11], donde en general, se le comunica al usuario que debe actualizar sus datos o de lo contrario perderá el servicio.

Lo mencionado en los apartados anteriores son solo métodos para extraer información ya que su motivación principal es el dinero, por lo tanto los datos que se extraen con más frecuencia son: números de cuentas bancarias, números de tarjetas de créditos o también cobrar por servicios que no tiene.

6. CONOCIENDO A LAS VÍCTIMAS

Se puede definir "víctima" como se argumenta en el diccionario de la RAE: "la persona que sufre un daño o perjuicio, que es provocado por una acción u omisión, ya sea por culpa de otra persona, o por fuerza mayor".

Con la intensión de separar los roles que puede cumplir una persona que está siendo atacada mediante el uso de la ingeniería social, estos se explican a continuación para facilitar su entendimiento y de esta forma poder evitar caer en dichos roles: El primer escenario es donde se trata a la persona como un canal o un medio para conseguir un objetivo, aquí el ingeniero social usa a la persona para extraer información de un sistema o en el mejor de los casos acceso al mismo y el segundo escenario es donde el objetivo principal son las personas, lo que busca es obtener información de ellas o que realicen alguna acción con el fin de obtener dinero, los números de tarjetas de crédito, débito, datos bancarios es la información más buscada, pero también el acceso a cuentas de correo electrónico y redes sociales ya que este tipo de cuentas tiene un buen valor en el mercado negro hasta 100$ dólares. Un ejemplo claro es cuando se recibe un mensaje de texto haciendo ganador de un gran premio en efectivo a quien lo recibe pero debe consignar cierto valor para reclamarlo diciendo que son para "tramites y papelería".

La Ingeniería Social ha trascendido en el tiempo debido a su efectividad para recolectar información personal o de entidades, por la tanto se han realizado estudios en los cuales se determinan los hábitos mínimos de seguridad que las personas tienen para proteger su información personal, familiar, laboral entre otros.

Con base en los resultados surgió la idea de hacer un estudio en la ciudad de Medellín con personas de diferentes estratos sociales y niveles de educación, para determinar cómo son los hábitos mínimos de seguridad en una ciudad que pertenece a un país en vías de desarrollo y que está entrando al mundo de las TIC.

Para conocer a fondo esta problemática y descubrir por qué la ingeniería social es tan efectiva, se realizó una encuesta sobre un grupo de 97 personas de diferentes disciplinas (médicos, abogados, ingenieros) con el objetivo de conocer sus hábitos informáticos.

La encuesta se realizó entre hombres y mujeres de 18 a 50 años, con la intención de separar los grupos y saber si se es más vulnerable en cierta edad o género. También se buscó conocer sus costumbres en las redes sociales, manejo de información entre muchos otros aspectos.

A. Preguntas y Hallazgos

Los resultados mostrados a continuación solo detallan las cifras que representan un riesgo para la seguridad informática de los usuarios de internet.

¿En qué lugar acceden con más frecuencia sus redes sociales y correo electrónico?

- Alrededor del 8.3 % de las personas encuestadas entran a sus diferentes cuentas de correo, bancos y redes sociales en lugares públicos.

Los establecimientos que proporcionan acceso a internet, también conocidos como cate internet son sitios donde muchas personas aceden a sus cuentas

de correo electrónico e incluso a banca en línea, esto es aprovechado por personas mal intencionadas para instalar programas que son capaces de capturar todas las contraseñas (keylogger) y enviar los datos a un correo electrónico controlado por el delincuente informático que recolecta la información.

¿Tiene restricciones en su perfil de red social (facebook, twitter) a su información personal?

- Un 21.7% dice no tener ningún tipo de restricción en su cuenta.

¿Acepta invitaciones en las redes sociales de personas desconocidas?

- Un 10.31% de los encuestados asegura aceptar invitaciones de personas desconocidas en redes sociales.

Análisis de las preguntas anteriores: Es un riesgo porque personas inescrupulosas pueden usar toda esa información para hacer suplantación de identidad e incluso robar la cuenta para su propio beneficio. El costo de una cuenta puede llegar hasta los $100 haciendo el robo de cuentas un negocio lucrativo, esto es debido a que esas cuentas son usadas para enviar virus o propagandas a otras cuentas.

¿Tiene cuidado en la información que publica en la red (fotos, información personal, transferencia de archivos)?

- Un poco más del 21% de las personas no cuidan a cuidan algunas veces la información que colocan en la red.

Se debe tener mucho cuidado con la información que pone en la red, porque esta información puede y será vista por cualquier persona que tenga una conexión a internet. En muchas ocasiones esta información es usada por delincuentes informáticos para hacer suplantación, robo de identidad, secuestros y robo de cuentas e incluso en algunos casos robo de dinero cuando colocan fotos de tarjetas de crédito o débito en sus cuentas de twitter.

¿Cuándo cierra sesión de sus cuentas de correo, redes sociales y demás programas, selecciona?

- Alrededor de un 13% (13.40) no cierran sesión o solo cierran la ventana del navegador.

Al no cerrar de forma correcta la sesión (opción cerrar cesión) cuando se termina de trabajar con las diferentes cuentas en la red, se presta para alguien más que tenga acceso al mismo equipo pueda entrar sin saber nada de nosotros o tener conocimiento en seguridad informática.

¿Usted es el único que tiene acceso a su correo electrónico?

- El 19.6% comparte el acceso de su cuenta con otra(s) persona(s).

El compartir el acceso no es un problema en si mismo ya que son personas de confianza, el problema surge cuando se pierde y estas personas pueden llegar a vengarse.

¿Usa la misma contraseña para sus diferentes cuentas de correo electrónico, redes sociales y computador?

- Casi un 40% usan la misma contraseña sobre sus diferentes cuentas de correo, redes sociales y de más servicios de internet.

Al tener la misma contraseña para todos los servicios que se tengan en la nube, permite que un delincuente informático al lograr entrar en una de las cuentas tenga acceso a las demás.

¿Anota sus contraseñas en un lugar visible para otras personas?

- Un poco más del 7% anotan sus contraseñas en lugares accesibles o visibles para otras personas.

Este mal hábito puede ocasionar que una persona mal intencionada por venganza o solo por hacer el daño puede entrar en dichas cuentas y borrar correos incluso hacer suplantación de identidad.

¿Utiliza información personal (cedula, fechas especiales, nombre de familiares o mascotas) en sus contraseñas?

- Alrededor de un 58% usa información personal para crear sus contraseñas.

Por lo general se usan: número de cedula, fechas especiales, nombre de familiares, nombres propios o mascotas en sus contraseñas (Maria1983). Esto hace que alguien que tenga acceso a estos datos (google, facebook, twitter), pueda entrar fácilmente.

¿Usa usted antivirus en su equipo personal?

- Un 27% no usan o solo usan algunas veces antivirus en sus equipos.

¿Si la licencia de su antivirus caduca usted la renueva?

- Más de un 40% no renueva la licencia cuando esta caduca.

Conclusión de las 2 preguntas anteriores: Esto hace que los diferentes tipos de malware puedan entrar con facilidad en los equipos y robar toda la información que contengan; además que alrededor de un 27% de las personas encuestadas descargan archivo de sus correos sin conocer su procedencia haciéndole el trabajo más fácil a los maleantes.

¿Sabe cómo darle seguridad a sus datos digítales (selección múltiple)?

- 67% indica el porcentaje de personas que no protegen de ninguna forma sus datos digitales (encriptar o contraseña en sus archivos).

Si un virus o cualquier tipo de malware logran entrar en el equipo de uso personal, la más posible es que robe información importante, pero si está protegida de alguna manera, se evita que el delincuente informático saque provecho al no poder acceder a ella.

¿Alguna vez ha sido estafado o engañado mediante uso de tecnologías digitales (selección múltiple)?

- Uno de las estadísticas más preocupantes es que el 33% de los encuestados ya ha sido víctima de alguna estafa electrónica donde la que más resalta es el engaño mediante mensajes de texto (smishing).

El ingeniero social se aprovecha de que a las personas les gusta ganar algo a cambio de poco, por esta razón la estrategia de usar los mensajes de texto donde quien los recibe se hace ganador de un gran premio y para hacerlo efectivo debe enviar una pequeña suma de dinero para efecto de trámites se atan efectiva.

¿Usa la opción de guardar contraseña en su cuenta de red social o correo electrónico en equipos que no sean suyos?

- Un 15.4% de las personas encuestadas aseveran usar la opción de guardar contraseña en equipos que no son de confianza.

Al guardar las contraseñas en equipos ajenos o que no son de nuestra confianza se puede estar dando acceso a datos a personas extrañas solo abrir el navegador.

¿Cada cuánto cambia su contraseña su cuenta de red social, correo electrónico o equipo de trabajo?

- Más de la mitad de las personas (52.6%) NUNCA cambian sus contraseñas y el 28% lo hace cada 6 meses.

Surgen 2 problemas graves, el primero es que un delincuente informático que quiere acceder a una cuenta de correo electrónico o red social, va a tener todo el tiempo del mundo para lograrlos y el segundo es que cuando lo logre podrá acceder a ella cuando quiera.

¿Capacita y acompaña a sus hijos en el uso de internet redes sociales, correo electrónico, video llamadas, etc.?

- Del 100% de las persona encuestadas el 21.65% no aplicaban o tenían hijos, de los demás encuestados se encontró que solo el 43% dijo hacerlo.

Una persona inescrupulosa puede aprovechar la falta de acompañamiento de los padres para obtener información sensible de ellos a través de sus hijos o en el peor de los casos fotos o una cita con ellos.

B. Resultados según el género.

Siguiendo con los hallazgos, se hizo una comparación entre hombres y mujeres, de los cuales 49.5% son mujeres y 50.5% hombres. Aunque la encuesta pregunta la edad NO se hizo una comparación por que las costumbres y hábitos no cambian o cambian muy poco al largo del tiempo haciendo que los resultados sean iguales a cualquier edad.

Los hombres son un poco más precavidos al momento de acceder a sus cuentas en sitios que no son de confianza con un 6% frente a un 13% de las mujeres.

Cuando de limitar el acceso a sus cuentas de red social se trata las mujeres mantiene un perfil muy bajo con un solo 6% que no lo hacen, mientras que los hombres tienen un alto 33%.

Al momento de tener cuidado con la información que colocan en la red es un poco más parejo un 15% de las mujer frente a un 24% de los hombres que no tiene cuidado con lo que suben.

Decir que un 13% de las mujeres contra un 2% de los hombres, se está comparando quien es menos cuidadoso en anotar sus contraseñas en un lugar visible para otras personas.

El 21% de las mujeres y el 33% de los hombres aseguran no tener instalado un antivirus en sus equipos personales e igual porcentaje al momento de descargar archivos de dudosa procedencia, haciendo que los delincuentes informáticos se esfuercen muy poco para conseguir lo que quieren.

7. RECOMENDACIONES Y CONCLUSIONES

1. *No consultar información sensible o personal en lugares como los café internet o sitios públicos:*

Los café internet son lugares muy concurridos donde muchas personas aceden a sus diferentes cuentas en la red, esto es aprovechado por los delincuentes informáticos para instalar keyloggers y demás

programas para obtener la información de las personas que acceden en estos sitios. También se corre el riesgo si se acede en sitios donde tengan "wifi gratis" porque existen programas que permiten a estos delincuentes ver la información que pasa por la red.

2. Cerrar sesión:
Si no se cierra la sesión debidamente (opción cerrar sesión) esta puede quedar activa, ósea que alguien no deseado con solo abrir nuevamente el navegador o darle la opción a tras puede entrar nuevamente sin problemas.

3. Evitar a toda costa invitaciones de personas desconocidas en redes sociales o mensajería instantánea:
Estas personas no siempre (nunca) tienen buenas intenciones, en ocasiones lo único que desean es obtener información del perfil y sacar provecho (robo de identidad, robo de cuenta, etc.), y con la mensajería instantánea quieren saber si el correo existe o vender servicios por lo general membrecías a páginas con contenido para adultos.

4. Usar múltiples contraseñas:
Los más común es tener por lo menos una cuenta de correo electrónico, cuentas en diferentes redes sociales y para todas ellas se usa la misma contraseña, esto puede ser un problema al momento en que si un atacante obtiene acceso a una cuenta tiene acceso a todas, además de esto se deberían cambiara al menos cada 3 meses.

5. Uso de contraseñas fuertes:
Para crear contraseñas seguras solo hay que hacer lo siguiente: pensar en algo que nos es familiar y no debe tener nombres propios, familiares, de mascotas, fechas especiales, como por ejemplo si hay mascotas en el hogar se puede crear algo así Tengo[3]gatoS es fácil de recordar, incluye caracteres alfanuméricos, caracteres especiales y más de 10 caracteres.

6. Uso de antivirus:
Tener y mantener el antivirus de nuestros computadores actualizado y funcionando es importante para protegerse de cualquier virus que pueda entras a través del navegador, memorias extraíbles o archivos adjuntos.

7. Correo electrónico no deseado
En ocasiones llega correo electrónico de bancos, servicios de mensajería, concursos donde en general, piden datos personales con la excusa de actualización de datos. Este tipo de correos se caracterizan por: venir en idiomas diferentes al nuestro, piden datos personales lo que en general ninguna entidad hace, traen amenazas en cancelar el servicio de no hacer lo que se pide, para evitar caer en este tipo de fraudes se aconseja digitar manualmente la dirección en el navegador www.entidad.com.

8. Ganar premio sin participar:
No responda mensajes de texto de ninguna índole e incluso llamadas, en donde le digan que se ha ganado un premio de un concurso en el cual no ha participado, y si lo ha hecho sospeche cuando le exijan dinero o algo más para reclamarlo.

9. Cuidar a sus hijos:
Es bueno saber que hacer hacen los hijos en internet, así protegemos los datos en los equipos, en el computador y lo más importante los hijos.

REFERENCIAS

[1] Shodan. "El Pirata Guason". Online [Abril, 2013]
[2] Kyron. "Whois". Online [Abril, 2013]
[3] Wikipedia. "Puerto informática". Online [Abril, 2013]
[4] Dragonjar. "Conceptos CHE". Online [Abril, 2013]
[5] Ordenadores y portátiles. "FTP". Online [Abril, 2013]
[6] Microsoft. "FTP". Online [Abril, 2013]
[7] PandaLabs. "Troyano". Online [Abril, 2013]
[8] Segu-Info. "Encuesta phishing". Online [Abril. 2013]
[9] Av-comparatives. "IT Secutiry Survey 2013". Online [Abril, 2013]
[10] UNAM. "Malware". Online [Abril, 2013]
[11] Infospyware. "Phishing". Online [Abril, 2013]